DISCRIMINANTS OF CHEBYSHEV RADICAL EXTENSIONS

THOMAS ALDEN GASSERT

Abstract. Let t be any integer and fix an odd prime ℓ. Let $\Phi(x) = T_\ell^n(x) - t$ denote the n-fold composition of the Chebyshev polynomial of degree ℓ shifted by t. If this polynomial is irreducible, let $K = \mathbb{Q}(\theta)$, where θ is a root of Φ. A theorem of Dedekind's gives a condition on t for which K is monogenic. For other values of t, we apply the Montes algorithm to obtain a formula for the discriminant of K and to compute basis elements for the ring of integers $\mathcal{O}_K$.

1. Introduction

Let $k = \mathbb{Q}(\theta)$ be a number field where θ is the root of a monic, irreducible polynomial $f(x) \in \mathbb{Z}[x]$. A classical problem in number theory is the determination of the discriminant of such a number field k, which is closely related to the discriminant of the polynomial $f(x)$ (see equations (1.1), (1.2), (1.3)). In this paper we focus on number fields that arise from iterating a particular family of polynomials, namely the Chebyshev polynomials (of the first kind), which we define in section 2. We use the standard notation from dynamics to denote the iterates of a polynomial:

Notation 1. Let $f \in \mathbb{Q}[x]$ be a polynomial of degree at least 2. Define $f^n(x) = f(f^{n-1}(x))$ to be the n-fold iterate of $f(x)$ under composition with $f^0(x) = x$. An exponent after the argument will be used to denote the n-th product, i.e. $f(x)^n := \big(f(x)\big)^n$.

The polynomials of interest are the iterates $T_\ell^n(x) - t$ where $T_d(x)$ is the Chebyshev polynomial of degree d, ℓ is an odd prime, and t is a fixed integer for which every iterate is irreducible. It is known that for every ℓ there are infinitely many values t for which the iterates $T_\ell^n(x) - t$ are all irreducible [4]. For example, when $\nu_\ell(t) = 1$, the polynomials are Eisenstein at ℓ (Lemma 2.2). A root θ_n of $T_\ell^n(x) - t$ is what we call a *Chebyshev radical*, and we call the number field $\mathbb{Q}(\theta_n)$ a *Chebyshev radial extension*. We remind the reader of the standard discriminant formulas.

Notation 2. Let $k = \mathbb{Q}(\theta)$ be a number field where θ is the root of a monic, irreducible polynomial $f(x) \in \mathbb{Z}[x]$, as originally defined. We write $D(f)$ for the discriminant of the polynomial and $\Delta(k)$ for the discriminant of the number field. These discriminants are given by

$$D(f) = \prod_{1 \le i < j \le d} (\theta_j - \theta_i)^2 \tag{1.1}$$

where f has roots $\theta_1, \dots, \theta_n$, and

$$\Delta(k) = \det(\mathrm{tr}_{k/\mathbb{Q}}(\alpha_i \alpha_j)) \tag{1.2}$$

where $\alpha_1, \dots, \alpha_d$ is a basis for the ring of integers $\mathcal{O}_k$.

The discriminant provides, in some sense, a measure of the arithmetic complexity of the underlying ring: $\mathbb{Z}[\theta]$ in the case of $D(f)$, and $\mathcal{O}_k$ in the case of $\Delta(k)$. Furthermore, $\mathbb{Z}[\theta] \subset \mathcal{O}_k$, and the discriminant scales as a square relative to the index $[\mathcal{O}_k : \mathbb{Z}[\theta]]$, for which we write

$$(\mathrm{ind}(f))^2 := [\mathcal{O}_k : \mathbb{Z}[\theta]]^2 = \frac{D(f)}{\Delta(k)}. \tag{1.3}$$

Date: April 23, 2013.

Notation 3. For simplicity, we will write $\Phi(x) := T_\ell^n(x) - t$ where ℓ, n, and t are understood to satisfy the properties listed above. Unless otherwise stated, we use θ to denote a root of Φ, and we write $K := \mathbb{Q}(\theta)$.

In this paper we work towards an alternative formula for $\Delta(K)$. A simple formula for $D(\Phi)$ depending only on ℓ and t is known (Proposition 2.9), leaving the majority of this paper to determine $\operatorname{ind}(\Phi)$. In section 3, we use Dedekind's criterion to identify the exact conditions under which a prime p divides $\operatorname{ind}(\Phi)$ (Theorem 3.5). In particular, these conditions precisely identify the values t for which the number field K is monogenic, that is $\mathcal{O}_K = \mathbb{Z}[\theta]$. The primes that divide $\operatorname{ind}(\Phi)$ fall into two categories:

(1) $\ell \mid \operatorname{ind}(\Phi)$ if and only if $\Phi(t) \equiv 0 \pmod{\ell^2}$
(2) $p \mid \operatorname{ind}(\Phi)$ if and only if $t \equiv \pm 2 \pmod{p^2}$.

In section 4, we introduce the Montes algorithm [5, 6, 7] for computing $\operatorname{ind}(f)$. In section 5, we apply the algorithm to the case where $\Phi(t) \equiv 0 \pmod{\ell^2}$ but $t \not\equiv \pm 2 \pmod{\ell^2}$ and obtain a closed formula for $\Delta(K)$ (Corollary 5.10). Additionally, in section 7, we determine generators for the ring of integers $\mathcal{O}_K$ when t is subjected to the same constraints (Theorem 7.1). In section 6, we give a conjecture for $\Delta(K)$ when t is odd and $t \not\equiv \pm 2 \pmod{\ell^2}$ (Conjecture 6.5). Most of our results are accompanied by examples.

2. Preliminaries: Properties of Chebyshev polynomials

We begin by recalling, without proof, some of the properties of Chebyshev polynomials (of the first kind) $T_d(x)$ and (of the second kind) $U_d(x)$ (e.g. see Rivlin [11] or Silverman [12]).

(1) For each integer $d \geq 0$, $T_d(x) \in \mathbb{Q}[x]$ is the unique monic polynomial satisfying
$$T_d(z + z^{-1}) = z^d + z^{-d}$$
in the field $\mathbb{Q}(z)$. Moreover, $T_d(x)$ is a degree d polynomial with integral coefficients.

(2) For each integer $d \geq 0$,
$$U_d(x) = \frac{d}{dx}\frac{T_{d+1}(x)}{d+1}$$
is a monic, integral polynomial of degree d.

(3) $T_d(T_e(x)) = T_{de}(x)$ for all $d, e \geq 0$.

(4) $T_d(-x) = (-1)^d T_d(x), \quad U_d(-x) = (-1)^d U_d(x)$.

(5) For all $d \geq 0$, the Chebyshev polynomials satisfy the recurrence relation
$$T_{d+2}(x) = xT_{d+1}(x) - T_d(x), \qquad U_{d+2}(x) = xU_{d+1}(x) - U_d(x).$$

(6) For all $d \geq 0$, the Chebyshev polynomials satisfy the trigonometric relations
$$T_d(2\cos(\theta)) = 2\cos(d\theta), \qquad U_d(2\cos(\theta)) = \frac{\sin((d+1)\theta)}{\sin(\theta)}.$$

(7) For all $d \geq 1$, the Chebyshev polynomials are given by the explicit formulas
$$T_d(x) = \sum_{k=0}^{\lfloor d/2 \rfloor} (-1)^k \frac{d}{d-k}\binom{d-k}{k} x^{d-2k}, \qquad U_d(x) = \sum_{k=0}^{\lfloor d/2 \rfloor} (-1)^k \binom{d-k}{k} x^{d-2k}.$$

(8) Equivalently,
$$U_d(x) = \frac{\left(x + \sqrt{x^2-4}\right)^{d+1} - \left(x - \sqrt{x^2-4}\right)^{d+1}}{2^{d+1}\sqrt{x^2-4}} \quad \text{if} \quad x \neq \pm 2.$$

We proceed with some results regarding the factorization of Chebyshev polynomials.

Lemma 2.1. If d is an odd integer and $t = \pm 2$, then

$$T_d(x) - t = (x - t)g(x)^2$$

for some monic polynomial $g(x) \in \mathbb{Z}[x]$ of degree $(d-1)/2$. Moreover, if $d = \ell^n$ for an odd prime ℓ, then $T_\ell^n(x) - t$ factors into irreducibles as

$$T_\ell^n(x) - t = (x - t)\phi_1(x)^2 \cdots \phi_n(x)^2$$

where $\phi_i(x)$ has degree $(\ell^i - \ell^{i-1})/2$.

Proof. Suppose $t = 2$. Recall that the Chebyshev polynomials satisfy the trigonometric relations

$$T_d(2\cos(\theta)) - 2 = 2\cos(d\theta) - 2 \quad \text{and} \quad U_{d-1}(2\cos(\theta)) = \frac{\sin(d\theta)}{\sin(\theta)},$$

and note that

$$\frac{d}{dx}\Big(T_d(x) - 2\Big) = dU_{d-1}(x).$$

Certainly, 2 is a root of $T_d(x) - 2$, and

$$\theta_i = 2\cos\left(\frac{2i\pi}{d}\right); \quad i = 1, \ldots, \frac{d-1}{2}$$

are roots of $T_d(x) - 2$ and its derivative. It follows that

$$T_d(x) - 2 = (x - 2)\prod_{i=1}^{(d-1)/2}(x - \theta_i)^2.$$

A similar argument applies in the case $t = -2$.

The factorization of $T_\ell^n(x) - t$ follows from the fact that the splitting field of $T_\ell^n(x) - t$ is $\mathbb{Q}(\zeta_{\ell^n})^+$, the maximal totally-real subfield of $\mathbb{Q}(\zeta_{\ell^n})$. □

Recall our previously defined notation $\Phi(x) = T_\ell^n(x) - t$.

Lemma 2.2. $\Phi(x) \equiv (x - t)^{\ell^n} \pmod{\ell}$.

Proof. Recall that

$$T_\ell(x) = \sum_{k=0}^{\lfloor \ell/2 \rfloor}(-1)^k \frac{(\ell - k - 1)!}{k!(\ell - 2k)!}\ell x^{\ell - 2k}.$$

Note that

$$\nu_\ell\left(\frac{(\ell - k - 1)!}{k!(\ell - 2k)!}\ell\right) = \begin{cases} 0 & \text{if } k = 0 \\ 1 & \text{otherwise,} \end{cases}$$

where ν_ℓ is the standard ℓ-adic valuation, and thus $T_\ell(x) \equiv x^\ell \pmod{\ell}$. It follows that

$$T_\ell^n(x) - t \equiv x^{\ell^n} - t \equiv (x - t)^{\ell^n} \pmod{\ell}.$$

□

Notation 4. We use $\bar{}$ to denote reduction modulo a prime p.

Proposition 2.3. Let p be an odd prime different from ℓ such that $t \equiv \pm 2 \pmod{p^2}$. Let μ be the least positive integer for which $\nu_\ell(p^{2\mu}-1) \geq 1$, and define $h = \nu_\ell(p^{2\mu}-1)$.

If $1 \leq n < h$, then $\overline{\Phi}(x)$ has $(\ell^n-1)/2\mu$ distinct irreducible factors of degree μ. That is,

$$\Phi(x) \equiv (x-\overline{t}) \prod_{i=1}^{\frac{\ell^n-1}{2\mu}} \phi_i(x)^2 \pmod{p},$$

where the ϕ_i's are distinct irreducible factors of degree μ.

Otherwise, if $n = h+e \geq h$, $\overline{\Phi}(x)$ has $(\ell^h-1)/2\mu$ distinct irreducible factors of degree μ, and ℓ^{h-1} distinct irreducible factors of degree $\ell^j\mu$ for each integer $1 \leq k \leq e$. More precisely,

$$\Phi(x) \equiv (x-\overline{t}) \prod_{i=1}^{\frac{\ell^{h-1}-1}{2\mu}} \phi_i(x)^2 \prod_{j=1}^{\frac{\ell^{h-1}(\ell-1)}{2\mu}} \prod_{k=0}^{e} \psi_j(T_\ell^k(x))^2 \pmod{p},$$

where the ψ_j's are irreducible factors of $\overline{T_\ell^h(x)-t}$ of degree μ, distinct from the ϕ_i's.

Remark 1. We will need to set up the tools for the proof of this proposition. The heuristic for the proof is the following: to every root θ of $\overline{\Phi}$ we assign a weight $w = [\mathbb{F}_p(\theta) : \mathbb{F}_p]$. If we can determine the weights of all the roots of $\overline{\Phi}$, then we know the degrees of the irreducible factors of $\overline{\Phi}$. The results from [4] describe the weights completely. We provide some terminology to understand the results in that paper.

The action of the Chebyshev polynomial $T_\ell(x)$ (or any other polynomial) on a finite field $\mathbb{F}_p$ and its extensions can be realized in the form of a directed graph. Each value in the field corresponds to a vertex in the graph, and the graph contains a directed edge from β to α if and only if $T_\ell(\beta) = \alpha$. The preimages of any value α can be found by tracing backwards along the paths terminating at α.

Definition 2.4. The *backwards orbit* of α is the set of all preimages of α under iteration by $T_\ell(x)$. In general, we restrict our discussion to the preimages contained within a certain finite field, and we write

$$\overleftarrow{O}_\alpha(\mathbb{F}_{p^m}) := \{\theta \in \mathbb{F}_{p^m} : T_\ell^n(\theta) = \alpha, n \geq 1\}.$$

The elements in the backward orbit of α can be arranged into tree graphs attached to α. We use the following terminology to describe these trees.

Definition 2.5. The *root* r of a directed tree graph is a specialized point in the graph towards which all edges are directed. The *height* of any vertex v is the length of the (unique) path from v to r. If the graph is finite, then the height of the graph is the length of the longest path contained in the graph. The vertices of a tree that have no incoming edges are often called *leaves*. A tree is called *n-ary* if every vertex that is not a leaf has n incoming edges. We say that an n-ary tree is *complete* n-ary if the height of every leaf is equal to the height of the graph.

Theorem 2.6 ([4], Theorem 2.6)**.** If ℓ is an odd prime and $\nu_\ell(p^{2m}-1) \geq 1$, then -2 and 2 are fixed and attached to each of these vertices are $(\ell-1)/2$ complete ℓ-ary trees of height $\nu_\ell(p^{2m}-1)-1$.

Lemma 2.7 ([4], Lemma 3.2)**.** Let μ be the least positive integer for which $\nu_\ell(p^{2\mu}-1) \geq 1$. If $\mu \mid m$, then

$$\nu_\ell(p^{2m}-1) = \nu_\ell(p^{2\mu}-1) + \nu_\ell(m).$$

We return to the proof of Proposition 2.3.

Proof. (Proposition 2.3) Recall that we defined μ to be the least positive integer for which $\nu_\ell(p^{2\mu}-1) \geq 1$, and we let $h = \nu_\ell(p^{2\mu}-1)$. Therefore, Theorem 2.6 implies that $\mathbb{F}_{p^\mu}$ is the minimal extension of $\mathbb{F}_p$ containing preimages of $\overline{t}$. A complete ℓ-ary tree of height $h-1$ contains $1+\ell+\cdots+\ell^{h-1} = \frac{\ell^h-1}{\ell-1}$ points, and thus

$$\#\overleftarrow{O}_{\overline{t}}(\mathbb{F}_{p^\mu}) = \frac{\ell-1}{2}\cdot\frac{\ell^h-1}{\ell-1} = \frac{\ell^h-1}{2}.$$

Each of these values is a root of an irreducible polynomial of degree μ, hence for $1 \leq n \leq h$, the degree of each of the irreducible factors of $\frac{\overline{T_\ell^n(x)-t}}{x-t}$ is μ. By Lemma 2.7, the smallest field containing all the roots of $\overline{T_\ell^{h+e}(x)-t}$ is $\mathbb{F}_{p^{\mu\ell^e}}$. It follows by induction that $\frac{\overline{T_\ell^{h+e}(x)-t}}{x-\overline{t}}$ has $\frac{\ell^h-\ell^{h-1}}{2\mu}$ factors of degree $\mu\ell^k$ for $1 \leq k \leq e$ and $\frac{\ell^h-1}{2\mu}$ factors of degree μ. □

Example 2.8. This example is meant as a illustrative description of the previous results. Consider the action of $T_5(x)$ on $\overline{\mathbb{F}}_7$, i.e. $\ell = 5$ and $p = 7$. One can verify that for this choice of primes, $\mu = 2$, $h = 2$, and $T_5(x) = (x \pm 2)(x^2 \mp x - 1)^2$ By Theorem 2.6, each of the two solutions to $x^2 \pm x - 1$ is the root of a complete 5-ary tree, and these roots are elements of $\mathbb{F}_{7^2}$. Moreover, this theorem and the associated lemma imply that every vertex at height $k \geq 1$ has weight $\mu\ell^{k-1}$. See Figure 1.

Lastly we provide a formula for the discriminant of $\Phi(x) = T_\ell^n(x) - t$. A general formula for the discriminant of an iterated polynomial is given by Aitken, Hajir, and Maire [1]. The following formula is a direct consequence of their result.

Proposition 2.9 ([4], Corollary 3.6.)**.** We have

$$D(\Phi) = \ell^{n\ell^n}(4-t^2)^{(\ell^n-1)/2}.$$

3. Monogenic number fields

In this section we identify sufficient conditions on t for which $\mathrm{ind}(\Phi) = 1$, or equivalently $D(\Phi) = \Delta(K)$. In particular, these are sufficient conditions for K to be a monogenic number field, meaning that the ring of integers $\mathcal{O}_K$ has a power basis. Our result gives rise to a large class of infinite towers of monogenic, and in general non-abelian, number fields. Consequently, for any (odd) prime ℓ and positive integer n, there are infinitely many monogenic number fields of degree ℓ^n. For a discussion of previous results regarding monogenic number fields, see Narkiewicz [10].

Definition 3.1. We say that an order $\mathcal{O} \subset \mathcal{O}_K$ is p-maximal if $p \nmid [\mathcal{O}_K : \mathcal{O}]$.

Our result is a consequence of the following theorem by Dedekind, which appears in Cohen [2].

Theorem 3.2 (Dedekind's criterion)**.** Let $\mathbb{Q}(\theta)$ be a number field, $T \in \mathbb{Z}[X]$ the monic minimal polynomial of θ and let p be a prime number. Denote by $\bar{}$ reduction modulo p. Let

$$\overline{T}(X) = \prod_{i=1}^{l} \overline{t_i}(X)^{e_i}$$

be the factorization of $T(X)$ modulo p in $\mathbb{F}_p[X]$, and set

$$g(X) = \prod_{i=1}^{l} t_i(X)$$

where the $t_i \in \mathbb{Z}[X]$ are arbitrary monic lifts of $\overline{t_i}$. Then

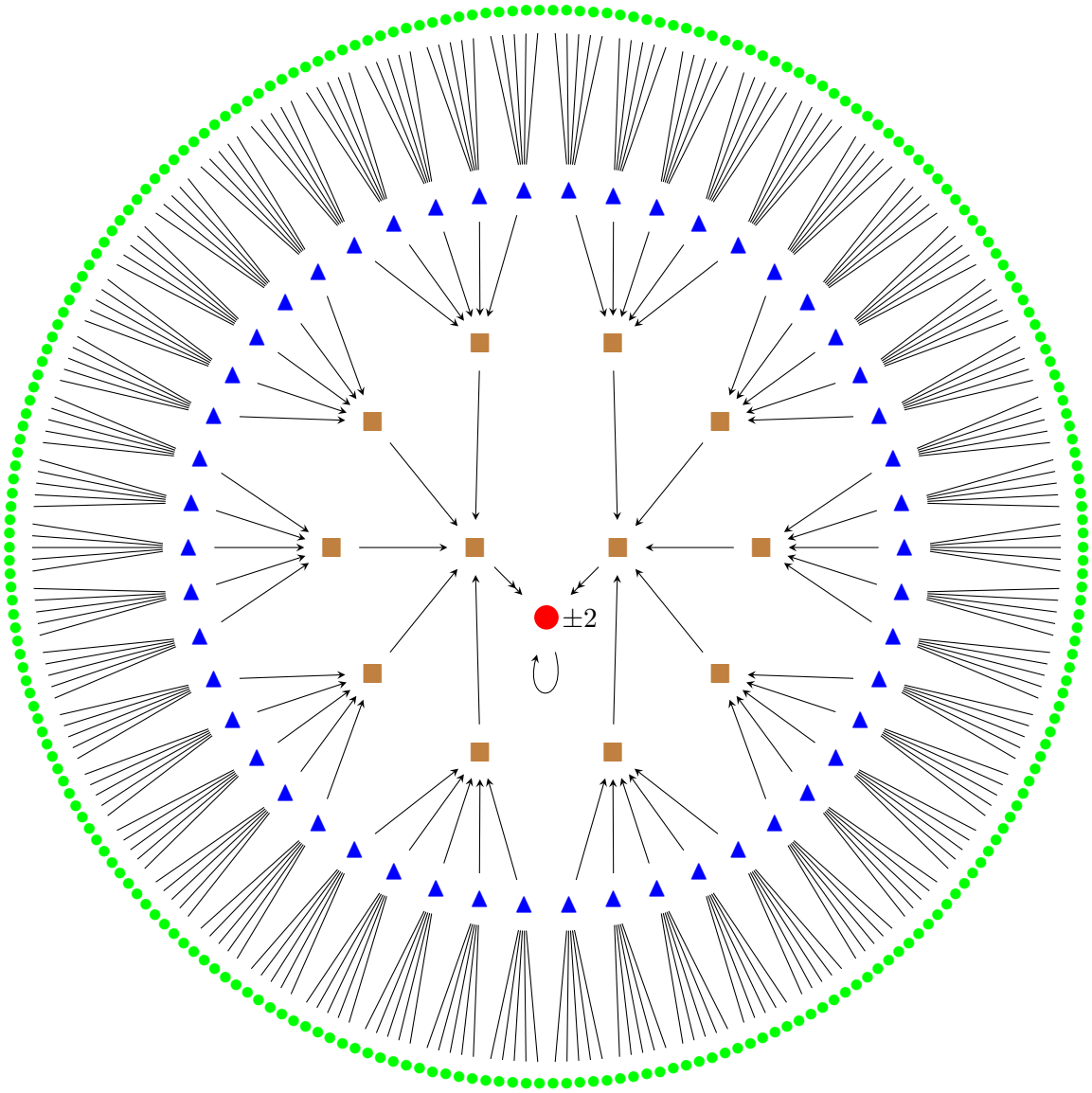

FIGURE 1. The roots of $T_5^4(x) - \overline{t}$ in $\overline{\mathbb{F}}_7$. A double arrow corresponds to the multiplicity of the preimage. The color and shape of the vertex corresponds to its weight: 1 (●); 2 (■); 10 (▲); 50 (●).

(1) The p-radical I_p of $\mathbb{Z}[\theta]$ at p is given by

$$I_p = p\mathbb{Z}[\theta] + g(\theta)\mathbb{Z}[\theta].$$

In other words, $x = A(\theta) \in I_p$ if and only if $\overline{g} \mid \overline{A}$.

(2) Let $h(X) \in \mathbb{Z}[X]$ be a monic lift of $\overline{T}(X)/\overline{g}(X)$ and set

$$f(X) = \frac{g(X)h(X) - T(X)}{p} \in \mathbb{Z}[X].$$

Then $\mathbb{Z}[\theta]$ is p-maximal if and only if $\gcd(\overline{f}, \overline{g}, \overline{h}) = 1$ in $\mathbb{F}_p[X]$.

(3) More generally, if U is a monic lift of $\overline{T}/(\overline{f},\overline{g},\overline{h})$ to $\mathbb{Z}[X]$, we have

$$\mathcal{O}' := \mathbb{Z}[\theta] + \frac{1}{p}U(\theta)\mathbb{Z}[\theta]$$

and if $m = \deg(\overline{f},\overline{g},\overline{h})$, then $[\mathcal{O}' \colon \mathbb{Z}[\theta]] = p^m$, hence $\operatorname{disc}(\mathcal{O}') = \operatorname{disc}(T)/p^{2m}$.

Remark 2. The ring $\mathcal{O}'$ in part (3) of Dedekind's criterion is subring of the ring of integers $\mathcal{O}_{\mathbb{Q}(\theta)}$. However, $\mathcal{O}'$ is not necessarily p-maximal, i.e. $[\mathcal{O}_K \colon \mathcal{O}']$ may be divisible by p.

We now work towards our main result regarding towers of monogenic extensions. The first result specifies conditions on t for which K is monogenic.

Theorem 3.3. If $\Phi(x) = T_\ell^n(x) - t$ is irreducible, then $D(\Phi) = \Delta(K)$ if and only if

(1) $\Phi(t) \not\equiv 0 \pmod{\ell^2}$ and
(2) both $t-2$ and $t+2$ are square-free.

Proof. Let θ be a root of Φ. The discriminants $\Delta(K)$ and $D(\Phi)$ are equal if and only if $\mathbb{Z}[\theta]$ is p-maximal for every prime p. We do not need to check every prime; the only primes for which $\mathbb{Z}[\theta]$ may not maximal are the primes that divide $D(\Phi)$ with multiplicity at least 2.

By Proposition 2.9, is sufficient to check ℓ and the primes that divide t^2-4.

We begin by using Dedekind's criterion to identify the condition on t for which $\mathbb{Z}[\theta]$ is ℓ-maximal. By Lemma 2.2,

$$\Phi(x) \equiv x^{\ell^n} - t \equiv (x-t)^{\ell^n} \pmod{\ell},$$

and we write

$$g(x) = x - t, \quad h(x) = (x-t)^{\ell^n - 1}, \quad f(x) = \frac{(x-t)^{\ell^n} - \Phi(x)}{\ell}.$$

The ring $\mathbb{Z}[\theta]$ is ℓ-maximal if and only if $\gcd(\overline{f},\overline{g},\overline{h}) = 1$, which holds if and only if t is not a root of $\overline{f}$ modulo ℓ. Evaluating $f(t)$, we see that

$$f(t) = \frac{\Phi(t)}{\ell} \not\equiv 0 \pmod{\ell}, \quad \text{and equivalently} \quad \Phi(t) \not\equiv 0 \pmod{\ell^2}.$$

Now, let p be a prime dividing t^2-4, i.e. $p \mid (t-2)(t+2)$. In this case, $t \equiv \pm 2 \pmod{p}$, and we write $\overline{t} \in \{2,-2\}$ for the reduction of t modulo p. By Lemma 2.1, we know that $\Phi(x) \equiv (x-\overline{t})\tau^2(x) \pmod{p}$ for some polynomial $\tau(x) \in \mathbb{F}_p[x]$. We seek to apply Dedekind's criterion, so we write

$$g(x) = (x-\overline{t})\tau(x), \quad h(x) = \tau(x), \quad f(x) = \frac{(x-\overline{t})\tau^2(x) - \Phi(x)}{p},$$

and proceed to show that $\gcd(\overline{f},\overline{g},\overline{h}) = 1$.

Let α be a root of τ. Then $\gcd(\overline{f},\overline{g},\overline{h}) = 1$ if and only if α is not a root of f modulo p. Evaluating f at α, we see that

$$f(\alpha) = -\frac{\Phi(\alpha)}{p} \equiv 0 \pmod{p} \quad \text{if and only if} \quad \Phi(\alpha) \equiv 0 \pmod{p^2}.$$

Recall that

$$T_\ell^n(\alpha) - \overline{t} \equiv \Phi(\alpha) \equiv (\alpha - \overline{t})\tau^2(\alpha) \equiv 0 \pmod{p},$$

and so $T_\ell^n(\alpha) \equiv \overline{t} \pmod{p}$. In particular, $-\Phi(\alpha) = t - T_\ell^n(\alpha) \equiv t - \overline{t} \pmod{p}$. Thus $\mathbb{Z}[\theta]$ is p-maximal if and only if $t - \overline{t} \not\equiv 0 \pmod{p^2}$, concluding the proof. □

The remainder of this section is dedicated to expanding this result.

Proposition 3.4. For any integers a and b,

$$T_\ell(a) \equiv T_\ell(b) \pmod{\ell^2} \text{ if and only if } a \equiv b \pmod{\ell}.$$

Proof. Suppose that $T_\ell(a) \equiv T_\ell(b) \pmod{\ell^2}$. By Lemma 2.2, $T_\ell(x) = x^\ell + \ell \cdot g(x)$, where $g(x)$ is a polynomial of degree $\ell - 2$. Hence

$$\begin{aligned} T_\ell(a) \equiv T_\ell(b) \pmod{\ell^2} &\Rightarrow a^\ell + \ell\, g(a) \equiv b^\ell + \ell\, g(b) \pmod{\ell^2} \\ &\Rightarrow a^\ell \equiv b^\ell \pmod{\ell} \\ &\Rightarrow a \equiv b \pmod{\ell}. \end{aligned}$$

For the converse statement, let $a \in \mathbb{Z}$ and write $a = q\ell + r$ such that $0 \le r < \ell$. It suffices to show that $T_\ell(a) \equiv T_\ell(r) \pmod{\ell^2}$.

$$\begin{aligned} T_\ell(a) = T_\ell(q\ell + r) &= \sum_{k=0}^{\lfloor \ell/2 \rfloor} (-1)^k \frac{(\ell - k - 1)!}{k!(\ell - 2k)!} \ell (q\ell + r)^{\ell - 2k} \\ &= \sum_{k=0}^{\lfloor \ell/2 \rfloor} (-1)^k \frac{(\ell - k - 1)!}{k!(\ell - 2k)!} \sum_{i=0}^{\ell - 2k} \binom{\ell - 2k}{i} q^i \ell^{i+1} r^{\ell - 2k - i} \\ &\equiv \sum_{k=0}^{\lfloor \ell/2 \rfloor} (-1)^k \frac{(\ell - k - 1)!}{k!(\ell - 2k)!} \ell r^{\ell - 2k} \\ &\equiv T_\ell(r) \pmod{\ell^2}. \end{aligned}$$

□

We are now ready to prove the main theorem of this section.

Theorem 3.5. If $\Phi(x) = T_\ell^n(x) - t$ is irreducible, then $D(\Phi) = \Delta(K)$ if and only if

(1) $T_\ell(t) - t \not\equiv 0 \pmod{\ell^2}$ and
(2) both $t - 2$ and $t + 2$ are square-free.

Proof. Note that for $n \ge 1$, $T_\ell^{n-1}(t) \equiv t^{\ell^{n-1}} \equiv t \pmod{\ell}$. By Proposition 3.4,

$$T_\ell^n(t) = T_\ell(T_\ell^{n-1}(t)) \equiv T_\ell(t) \pmod{\ell^2}.$$

Thus

$$T_\ell^n(t) \equiv t \pmod{\ell^2} \quad \text{if and only if} \quad T_\ell(t) \equiv t \pmod{\ell^2}.$$

The result is now an immediate consequence of Theorem 3.3. □

Remark 3. What we have shows is that the conditions for which $D(\Phi) = \Delta(K)$ only depend on ℓ and t. By picking a compatible sequence of preimages of t: $\{t = \theta_0, \theta_1, \ldots\}$ such that $T_\ell(\theta_n) = \theta_{n-1}$, we designate a tower of number fields

$$\mathbb{Q} \subset K_1 \subset K_2 \subset \cdots$$

where $K_n = \mathbb{Q}(\theta_n)$. By our result, K_1 is monogenic if and only if K_n is monogenic, and in particular we have identified a two parameter family of towers of monogenic number fields.

We conclude this section by identifying the values t for which $\Phi(t) \equiv 0 \pmod{\ell^2}$.

Theorem 3.6. $\Phi(t) \equiv 0 \pmod{\ell^2}$ if and only if $t \equiv T_\ell(a)$ for some $a \in \mathbb{Z}/\ell^2\mathbb{Z}$.

Proof. By the same argument in the proof of Theorem 3.5, it is sufficient to show that $T_\ell(t) \equiv t \pmod{\ell^2}$ if and only if $T_\ell(a) \equiv t \pmod{\ell^2}$ for some $a \in \mathbb{Z}/\ell^2\mathbb{Z}$.

Suppose there exists $a \in \mathbb{Z}/\ell^2\mathbb{Z}$ such that $T_\ell(a) \equiv t \pmod{\ell^2}$. By Lemma 2.2, $T_\ell(a) \equiv a \pmod{\ell}$, and so $a \equiv t \pmod{\ell}$. Thus, by Proposition 3.4

$$T_\ell(t) \equiv T_\ell(a) \equiv t \pmod{\ell^2}.$$

The converse statement is immediate by setting $a = t$. □

Remark 4. In fact, Proposition 3.4 implies that $T_\ell(x)$ is an ℓ-to-one map from $\mathbb{Z}/\ell^2\mathbb{Z}$ to $\mathbb{Z}/\ell^2\mathbb{Z}$ defined by $a + b\ell \mapsto T_\ell(a)$. Thus for every prime ℓ, there are exactly ℓ "bad" values for t modulo ℓ^2 for which K is not monogenic. These bad values are exactly the set of values

$$\{T_\ell(0), T_\ell(1), \ldots, T_\ell(\ell-1)\} \subset \mathbb{Z}/\ell^2\mathbb{Z}.$$

Corollary 3.7. For an arbitrary choice of t, the probability that $\ell \mid \mathrm{ind}(\Phi)$ is $1 - \ell^{-1}$.

4. Montes algorithm: Theorem of the index

The remainder of the paper is dedicated to studying the cases where $D(\Phi) \neq \Delta(K)$. This will happen whenever the conditions in Theorem 3.5 are relaxed, namely, if t is chosen so that $T_\ell(t) - t \equiv 0 \pmod{\ell^2}$, and/or at least one of $t-2$ and $t+2$ is not square-free. In this section we introduce the Montes algorithm for computing $\mathrm{ind}(f)$ that was recently developed by Guàrdia, Montez, and Nart [5, 6, 7], though we primarily follow the presentation found in the paper by el Fadil, Montez, Nart [3]. Their method employs a more refined variation of the Newton polygon, called the ϕ-Newton polygon, which captures arithmetic data attached to the irreducible factors ϕ of $\overline{\Phi}$.

Notation 5. We fix the following notation. Let p be a prime number and let $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial whose reduction modulo p is irreducible. We denote by $\mathbb{F}_\phi$ the finite field $\mathbb{Z}[x]/(p, \phi)$, and by

$$\overline{} : \mathbb{Z}[x] \to \mathbb{F}_p[x], \quad \mathrm{red} : \mathbb{Z}[x] \to \mathbb{F}_\phi$$

the respective homomorphisms of reduction modulo p and modulo $(p, \phi(x))$. We extend the usual p-adic valuation to polynomials by

$$\nu_p(c_0 + \cdots + c_r x^r) := \min_{0 \le i \le r} \{\nu_p(c_i)\}.$$

Any $f(x) \in \mathbb{Z}[x]$ admits a unique ϕ-adic development:

$$f(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_r(x)\phi(x)^r,$$

with $a_i(x) \in \mathbb{Z}[x]$ and $\deg(a_i) < \deg(\phi)$. To each coefficient $a_i(x)$ we attach the p-adic value

$$u_i = \nu_p(a_i(x)) \in \mathbb{Z} \cup \{\infty\}$$

and the point of the plane (i, u_i), if $u_i < \infty$.

Definition 4.1. The *ϕ-Newton polygon* of $f(x)$ is the lower convex envelope of the set of points $(i, u_i), u_i < \infty$, in the Euclidian plane. We denote this open polygon by $N_\phi(f)$.

The ϕ-Newton polygon is the union of different adjacent sides $S_1, \ldots, S_g$ with increasing slopes $\lambda_1 < \cdots < \lambda_g$. We shall write $N_\phi(f) = S_1 + \cdots + S_g$. The end points of the sides are called the vertices of the polygon.

Definition 4.2. The polygon determined by the sides of negative slope of $N_\phi(f)$ is called the *principal ϕ-polygon* of $f(x)$ and will be denoted by $N_\phi^-(f)$. The length, of $N_\phi^-(f)$, denoted $\ell(N_\phi^-(f))$, is always equal to the highest exponent a such that $\overline{\phi(x)}^a$ divides $\overline{f(x)}$ in $\mathbb{F}_p[x]$.

Notation 6. From now on, any reference to the ϕ-Newton polygon of $f(x)$ will be taken to mean the principal ϕ-polygon, and for simplicity, we will write $N_\phi(f) := N_\phi^-(f)$.

We attach to any abscissa $0 \le i \le \ell(N_\phi)$ the following residual coefficient $c_i \in \mathbb{F}_p[x]/(\phi)$.

$$c_i = \begin{cases} 0 & \text{if } (i, u_i) \text{ lies strictly above } N_\phi \text{ or } u_i = \infty, \\ \operatorname{red}(a_i(x)/p^{u_i}) & \text{if } (i, u_i) \text{ lies on } N_\phi. \end{cases}$$

Note that c_i is always nonzero in the latter case, because $\deg(a_i(x)) < \deg(\phi)$.

Let S be one of the sides of N_ϕ, with slope $\lambda = -h/e$, where e and h are relatively prime, positive integers. The length of S is the length, $\ell(S)$, of the projection of S to the horizontal axis, the degree of S is $d(S) := \ell(S)/e$, the ramification index of S is $e(S) := e$.

Definition 4.3. Let s be the initial abscissa of S, and let $d := d(S)$. We define the *residual polynomial* attached to S (or to λ) to be the polynomial

$$R_\lambda(f)(y) := c_s + c_{s+e}y + \cdots + c_{s+(d-1)e}y^{d-1} + c_{s+de}y^d \in \mathbb{F}_\phi[y].$$

Definition 4.4. Let $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial, irreducible modulo p. We say that $f(x)$ is *ϕ-regular* if for every side $N_\phi(f)$, the residual polynomial attached to the side is separable.

Choose monic polynomials $\phi_1(x), \ldots, \phi_t(x) \in \mathbb{Z}[x]$ whose reduction modulo p are the different irreducible factors of $\overline{f(x)} \in \mathbb{F}_p[x]$. We say that $f(x)$ is *p-regular* with respect to this choice if $f(x)$ is ϕ_i-regular for every $1 \le i \le t$.

Definition 4.5. The *ϕ-index* of $f(x)$ is $\deg \phi$ times the number of points with integral coordinates that lie below or on the polygon $N_\phi(f)$, strictly above the horizontal axis, and strictly to the right of the vertical axis. We denote this number by $\operatorname{ind}_\phi(f)$.

Notation 7. Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial and let θ be a root of $f(x)$. We denote by

$$\operatorname{ind}_p(f) := \nu_p([\mathcal{O}_{\mathbb{Q}(\theta)} \colon \mathbb{Z}[\theta]]),$$

the p-adic value of the index of the polynomial $f(x)$.

Theorem 4.6 ([7], section 4.4)**.** Theorem of the index:

$$\operatorname{ind}_p(f) \ge \operatorname{ind}_{\phi_1}(f) + \cdots + \operatorname{ind}_{\phi_t}(f),$$

and equality holds if $f(x)$ is p-regular.

5. Index calculations: On the multiplicity of ℓ

Recall that $\Phi(x) := T_\ell^n(x) - t$, and let θ be a root of Φ. In the proof of Theorem 3.3 we showed that $\mathbb{Z}[\theta]$ is ℓ-maximal if and only if $\Phi(t) \not\equiv 0 \pmod{\ell^2}$. Here, we relax this condition and study the effect on $\operatorname{ind}_\ell(\Phi)$. Specifically, in this section, we fix t so that $\Phi(t) \equiv 0 \pmod{\ell^2}$ *with the exception* that $t \not\equiv \pm 2 \pmod{\ell^2}$.

Following the prescription outlined in the previous section, we must start by factoring Φ modulo ℓ. Recalling Lemma 2.2:

$$\Phi(x) \equiv (x - t)^{\ell^n} \pmod{\ell}.$$

If $t \equiv 0 \pmod{\ell}$, then $\phi(x) = x$, and $N_\phi(\Phi)$ is just the usual Newton polygon of Φ. Otherwise, if $t \not\equiv 0 \pmod{\ell}$, then $\phi(x) = x - t$, and we must compute the ϕ-development of Φ. Note, however, that $N_\phi(\Phi)$ is the Newton polygon of the shifted Chebyshev polynomial $\Phi(\phi(x)+t)$ as a polynomial in $\phi(x)$. The following lemma will assist our calculations.

Definition 5.1. For any prime p and any integer a, the *p-adic expansion* of a is

$$a = a_0p^0 + a_1p^1 + a_2p^2 + \cdots + a_sp^s$$

with $0 \leq a_i < p$. We define the function

$$\sigma_p(a) = \sum_{i=0}^{\infty} a_i.$$

Lemma 5.2. Let p be a prime, and let σ_p be the function defined above.

(1) Let a and b be integers written in base p. The number of "carries" performed when summing $a + b$ in base p is

$$\#\text{carries} = \frac{\sigma_p(a) + \sigma_p(b) - \sigma_p(a+b)}{p-1}.$$

(2) $\nu_p(a) = \dfrac{1 + \sigma_p(a-1) - \sigma_p(a)}{p-1}$.

(3) $\nu_p(a!) = \dfrac{n - \sigma_p(a)}{p-1}$.

(4) (Kummer [8]) $\nu_p\binom{a+b}{b} = \#$carries in $a + b$ summed in base p.

Though these are well-known, for the convenience of the reader, we provide proofs, as they are short.

Proof. (1) Write a and b in their base p expansions: $a = \sum a_ip^i$ and $b = \sum b_ip^i$. If ever $c_i := a_i + b_i \geq p$, then perform a "carry": subtract p from c_i and add 1 to c_{i+1}, repeating until all c_i are less than p. These c_i are the coefficients for the base p expansion of $a + b$: $a + b = \sum c_ip^i$. Each carry reduces the sum $\sigma_p(a) + \sigma_p(b)$ by $p - 1$, and the result follows.

(2) This follows immediately from part (1). If k is the smallest integer for which $a - 1 \equiv -1 \pmod{p^k}$, then the sum $(a - 1) + 1$ requires k carries in base p.

(3) By part (2), we have the telescoping sum

$$\nu_p(a!) = \sum_{i=1}^{a} \nu_p(i) = \sum_{i=1}^{a} \frac{1 + \sigma_p(i-1) - \sigma_p(i)}{p-1} = \frac{a - \sigma_p(a)}{p-1}.$$

(4) By part (3)

$$\begin{aligned}\nu_p\binom{a+b}{b} = \nu_p\left(\frac{(a+b)!}{a!b!}\right) &= \nu_p((a+b)!) - \nu_p(a!) - \nu(b!) \\ &= \frac{a + b - \sigma_p(a+b)}{p-1} + \frac{a - \sigma_p(a)}{p-1} - \frac{b - \sigma_p(b)}{p-1} \\ &= \frac{\sigma_p(a) + \sigma_p(b) - \sigma_p(a+b)}{p-1}.\end{aligned}$$

The result follows from part (1).

□

We consider the case where $t \equiv 0 \pmod{\ell}$ and proceed by computing the Newton polygon of $T_\ell^n(x)$. We also write $T_\ell^n(x) = \sum_{k=0}^{\lfloor \ell^n/2 \rfloor} c_i x^{\ell^n - 2k}$ where

$$c_i := \frac{\ell^n}{\ell^n - (\ell^n - i)/2}\binom{\ell^n - (\ell^n - i)/2}{(\ell^n - i)/2} = \frac{2\ell^n}{\ell^n + i}\binom{(\ell^n + i)/2}{(\ell^n - i)/2}.$$

Proposition 5.3. For any integer $0 < i \leq \ell^m \leq \ell^n$, $\nu_\ell(c_i) \geq n - m$ with equality only if $i = \ell^m$. Furthermore, $N_\phi(T_\ell^n) = \sum_{m=1}^n S_m$ where S_m is the edge with endpoints $(\ell^{m-1}, n - m + 1)$ and $(\ell^m, n - m)$.

Proof. When $i = \ell^m$,

$$\nu_\ell(c_{\ell^m}) = n + \nu_\ell\binom{(\ell^n + \ell^m)/2}{(\ell^n - \ell^m)/2} - \nu_\ell(\ell^n + \ell^m).$$

Note that

$$\binom{(\ell^n + \ell^m)/2}{(\ell^n - \ell^m)/2} = \binom{(\ell^n + \ell^m)/2}{(\ell^n + \ell^m)/2 - (\ell^n - \ell^m)/2} = \binom{(\ell^n + \ell^m)/2}{\ell^m}.$$

The ℓ-valuation of this number can be determined using Lemma 5.2 by considering a sum in base ℓ. Writing

$$\frac{\ell^n + \ell^m}{2} - \ell^m = \frac{\ell - 1}{2} \cdot \ell^m + \frac{\ell - 1}{2} \cdot \ell^{m+1} + \cdots + \frac{\ell - 1}{2} \cdot \ell^n,$$

it is clear that $(\frac{\ell^n - \ell^m}{2} - \ell^m) + \ell^m$ requires no carries when summed in base ℓ. Thus

$$\nu_\ell\binom{(\ell^n + \ell^m)/2}{(\ell^n - \ell^m)/2} = 0.$$

Furthermore,

$$\nu_\ell(\ell^n + \ell^m) = \nu_\ell(\ell^m) + \nu_\ell(\ell^{n-m} + 1) = m,$$

proving that $\nu_\ell(c_{\ell^m}) = n - m$.

Suppose that $0 < i < \ell^m$. Then $\nu_\ell(\ell^n + i) = \nu_\ell(i) < m$, and

$$\nu_\ell(c_i) = n + \nu_\ell\binom{(\ell^n + i)/2}{(\ell^n - i)/2} - \nu_\ell(\ell^n + i) > n - m.$$

From the previous parts we conclude that the polygon $S_1 + \cdots + S_n$ is a lower boundary for the points $(i, \nu_\ell(c_i))$ with vertices at $(m, \nu_\ell(c_{\ell^m}))$. It is easily verified that this polygon is convex. Let λ_m denote the slope of S_m, which is given by

$$\lambda_m = \frac{-1}{\ell^{m-1}(\ell - 1)}.$$

Clearly, $\lambda_1 < \lambda_2 < \cdots < \lambda_n$. □

Knowing the Newton polygon for T_ℓ^n, we can determine the Newton polygon for Φ.

Proposition 5.4. Suppose $t \equiv 0 \pmod{\ell}$, and let $v = \nu_\ell(t)$. Let $S_m, m = 1, \ldots, n$ be the edges defined in the previous theorem. Define S' to be the edge with endpoints $(0, v)$ and $(\ell^{n-v+1}, v - 1)$. Then

$$N_\phi(\Phi) = S' + S_{n-v+2} + S_{n-v+3} + \cdots + S_n.$$

Proof. Let λ_m be the slope of S_m and λ' be the slope of S'. It suffices to show that $\lambda_{n-v+1} < \lambda' < \lambda_{n-v+2}$. This is easily verified:

$$\lambda_{n-v} = \frac{-1}{\ell^{n-v}(\ell - 1)} \quad < \quad \lambda' = \frac{-1}{\ell^{n-v+1}} \quad < \quad \lambda_{n-v+2} = \frac{-1}{\ell^{n-v+1}(\ell - 1)}.$$

□

Remark 5. Although we write $v = \nu_\ell(t)$, due to the nature of the coefficients of $\Phi(x)$ it would also have been correct to define $v = \nu_\ell(\Phi(t))$. We adopt this new definition of v for the remainder of this section.

We move on to the case where $\phi(x) = x - t$ and $t \not\equiv 0 \pmod{\ell}$ where we must determine the Newton polygon of $\Phi(x) = \Phi(\phi(x) + t)$ as a polynomial in $\phi(x)$. We proceed by determining the ϕ-development of $\Phi(x) = T_\ell^n(x) - t$.

$$\begin{aligned}
T_\ell^n(\phi+t) - t &= -t + \sum_{k=0}^{\lfloor \ell^n/2 \rfloor} (-1)^k \binom{\ell^n - k}{k} \frac{\ell^n}{\ell^n - k} (\phi+t)^{\ell^n - 2k} \\
&= -t + \sum_{k=0}^{\lfloor \ell^n/2 \rfloor} (-1)^k \binom{\ell^n - k}{k} \frac{\ell^n}{\ell^n - k} \sum_{i=0}^{\ell^n - 2k} \binom{\ell^n - 2k}{i} t^{\ell^n - 2k - i} \phi^i \\
&= -t + \sum_{i=0}^{\ell^n} \sum_{k=0}^{\lfloor (\ell^n - i)/2 \rfloor} (-1)^k \binom{\ell^n - k}{k} \binom{\ell^n - 2k}{i} \frac{\ell^n}{\ell^n - k} t^{\ell^n - 2k - i} \phi^i \\
&= -t + \sum_{k=0}^{\lfloor \ell^n/2 \rfloor} (-1)^k \binom{\ell^n - k}{k} \frac{\ell^n}{\ell^n - k} t^{\ell^n - 2k} \\
&\qquad + \sum_{i=1}^{\ell^n} \sum_{k=0}^{\lfloor (\ell^n - i)/2 \rfloor} (-1)^k \binom{\ell^n - k}{k} \binom{\ell^n - 2k}{i} \frac{\ell^n}{\ell^n - k} t^{\ell^n - 2k - i} \phi^i \\
&= T_\ell^n(t) - t + \sum_{i=1}^{\ell^n} \sum_{k=0}^{\lfloor (\ell^n - i)/2 \rfloor} (-1)^k \binom{\ell^n - k}{k} \binom{\ell^n - 2k}{i} \frac{\ell^n}{\ell^n - k} t^{\ell^n - 2k - i} \phi^i
\end{aligned}$$

For ease, we will write

$$b_i := \ell^n \sum_{k=0}^{\lfloor \frac{\ell^n - i}{2} \rfloor} (-1)^k \binom{\ell^n - k}{k} \binom{\ell^n - 2k}{i} \frac{t^{\ell^n - 2k - i}}{\ell^n - k}$$

denote the coefficient of ϕ^i for $1 \le i \le \ell^n$.

Lemma 5.5. For positive integers a, b, and c satisfying $0 \le b \le \frac{a-c}{2}$, the binomial coefficients satisfy the following relationship:

$$\binom{a-b}{b}\binom{a-2b}{c} = \binom{a-b-c}{b}\binom{a-b}{c}.$$

Proof.

$$\begin{aligned}
\binom{a-b}{b}\binom{a-2b}{c} &= \frac{(a-b)!}{b!(a-2b!)} \cdot \frac{(a-2b)!}{c!(a-2b-c)!} = \frac{(a-b)!}{c!(a-b-c)!} \cdot \frac{(a-b-c)!}{b!(a-2b-c)!} \\
&= \binom{a-b-c}{b}\binom{a-b}{c}.
\end{aligned}$$

□

This lemma allow us to rewrite b_i in a way that is better suited for our analysis:

$$b_i = \sum_{k=0}^{\lfloor \frac{\ell^n - i}{2} \rfloor} (-1)^k \frac{\ell^n}{\ell^n - k} \binom{\ell^n - k}{k} \binom{\ell^n - 2k}{i} t^{\ell^n - 2k - i}$$

$$= \frac{\ell^n}{i} \sum_{k=0}^{\lfloor \frac{\ell^n - i}{2} \rfloor} (-1)^k \binom{\ell^n - i - k}{k} \binom{\ell^n - k - 1}{i-1} t^{\ell^n - 2k - i}.$$

There are a couple more results that we will use to compute the valuations of the coefficients. The first is a result by Lucas [9].

Theorem 5.6 (Lucas)**.** Let p be a prime, and let $0 \leq m \leq n$ with $n = \sum_{j=0}^{l} n_j p^j$ and $m = \sum_{j=0}^{l} m_j p^j$. Then

$$\binom{n}{m} \equiv \prod_{j=0}^{l} \binom{n_j}{m_j} \pmod{p}.$$

We also use the following fact about Chebyshev polynomials (of the second kind) $U_d(x)$. Recall that $U_d(x)$ is given by the expression

$$U_d(x) = \frac{\left(x + \sqrt{x^2-4}\right)^{d+1} - \left(x - \sqrt{x^2-4}\right)^{d+1}}{2^{d+1}\sqrt{x^2-4}} \quad \text{if} \quad x \neq \pm 2.$$

Lemma 5.7. Let ℓ be an odd prime. If $x \not\equiv \pm 2 \pmod{\ell}$, then $U_{\ell-1}(x) \equiv \pm 1 \pmod{\ell}$.

Proof. A local calculation: Let $\alpha = \frac{x+\sqrt{x^2-4}}{2}$ and $\beta = \frac{x-\sqrt{x^2-4}}{2}$, and consider α and β as elements of $\mathbb{F}_{\ell^2}$. Here, the Frobenius map fixes $\mathbb{F}_\ell$, and acts by conjugation on its complement. Hence, if $\sqrt{x^2-4} \in \mathbb{F}_\ell$, then $\alpha^\ell = \alpha$ and $\beta^\ell = \beta$, so

$$U_{\ell-1}(x) = \frac{\alpha - \beta}{\sqrt{x^2-4}} = 1 \in \mathbb{F}_\ell.$$

Otherwise, if $\sqrt{x^2-4} \notin \mathbb{F}_\ell$, then $\alpha^\ell = \beta$ and $\beta^\ell = \alpha$, so

$$U_{\ell-1}(x) = \frac{\beta - \alpha}{\sqrt{x^2-4}} = -1 \in \mathbb{F}_\ell.$$

□

We proceed to compute the valuations of the coefficients b_i.

Proposition 5.8. Suppose that $t \not\equiv \pm 2 \pmod{\ell}$ and $\ell^m \leq i < \ell^{m+1} \leq \ell^n$. Then $\nu_\ell(b_i) \geq n - m$ with equality if $i = \ell^m$.

Proof. Assume first that $i = \ell^m + \varepsilon$ for some integer $0 < \varepsilon < (\ell-1)\ell^m$. We show that $\nu_\ell(b_i) \geq n - m$.

$$\begin{aligned}
b_i &= \frac{\ell^n}{\ell^m + \varepsilon} \sum_{k=0}^{\lfloor \frac{\ell^n - i}{2} \rfloor} (-1)^k \binom{\ell^n - i - k}{k} \binom{\ell^n - k - 1}{\ell^m + \epsilon - 1} t^{\ell^n - 2k - i} \\
&= \ell^n \sum_{k=0}^{\lfloor \frac{\ell^n - i}{2} \rfloor} (-1)^k \binom{\ell^n - i - k}{k} \frac{(\ell^n - k - 1)!}{(\ell^m + \varepsilon)!(\ell^n - \ell^m - k - \varepsilon)!} t^{\ell^n - 2k - i} \\
&= \ell^n \sum_{k=0}^{\lfloor \frac{\ell^n - i}{2} \rfloor} (-1)^k \binom{\ell^n - i - k}{k} \frac{(\ell^n - k - 1)!}{\ell^m(\ell^m - 1)!(\ell^n - \ell^m - k)!} \frac{\ell^m! \varepsilon!}{(\ell^m + \varepsilon)!} \frac{(\ell^n - \ell^m - k)!}{\varepsilon!(\ell^n - \ell^m - k - \varepsilon)!} t^{\ell^n - 2k - i} \\
&= \frac{\ell^{n-m}}{\binom{\ell^m + \varepsilon}{\ell^m}} \sum_{k=0}^{\lfloor \frac{\ell^n - i}{2} \rfloor} (-1)^k \binom{\ell^n - i - k}{k} \binom{\ell^n - k - 1}{\ell^m - 1} \binom{\ell^n - \ell^m - k}{\varepsilon} t^{\ell^n - 2k - i}.
\end{aligned}$$

The valuation of the sum is non-negative since it is an integer. Furthermore, $\nu_\ell\binom{\ell^m+\varepsilon}{\ell^m} = 0$ by Lemma 5.2 since $\ell^m + \varepsilon$ requires no carries in base ℓ. Thus $\nu_\ell(b_i) \geq n - m$.

Assume now that $i = \ell^m$. To show that $\nu_\ell(b_{\ell^m}) = n - m$, we show that $\ell^{m-n} b_{\ell^m}$ is relatively prime to ℓ. It suffices to sum over the terms that are relatively prime to ℓ and show that the sum of these terms is not divisible by ℓ. We write the following numbers in their base-ℓ expansions.

$$k = \sum_{j=0}^{n-1} k_j \ell^j; \qquad \ell^m - 1 = \sum_{j=0}^{m-1} (\ell - 1)\ell^j; \qquad \ell^n - k - 1 = \sum_{j=0}^{n-1} (\ell - k_j - 1)\ell^j.$$

By Theorem 5.6,

$$\begin{aligned}\binom{\ell^n - k - 1}{\ell^m - 1} &\equiv \binom{\ell - k_0 - 1}{\ell - 1} \cdots \binom{\ell - k_{m-1} - 1}{\ell - 1} \binom{\ell - k_m - 1}{0} \cdots \binom{\ell - k_{n-1} - 1}{0} \pmod{\ell} \\ &\equiv \begin{cases} 1 \pmod{\ell} & \text{if } k_0 = \cdots = k_{m-1} = 0 \\ 0 \pmod{\ell} & \text{otherwise.} \end{cases}\end{aligned}$$

That is, $\binom{\ell^n - k - 1}{\ell^m - 1}$ is relatively prime to ℓ if and only if $\ell^m \mid k$. We continue with the additional assumption that ℓ^m divides k. Now, the base-ℓ expansion of $\ell^n - \ell^m - k$ is

$$\ell^n - \ell^m - k = \sum_{j=m}^{n-1} (\ell - k_j - 1)\ell^j.$$

Applying Theorem 5.6 to the other binomial coefficient in the sum, we see that

$$\binom{\ell^n - \ell^m - k}{k} \equiv \binom{\ell - k_m - 1}{k_m} \cdots \binom{\ell - k_{n-1} - 1}{k_{n-1}} \pmod{\ell},$$

which is nonzero if and only if $0 \leq k_j \leq (\ell - 1)/2$ for each $j = m, m+1, \ldots, n-1$. We have the following:

$$\begin{aligned}\ell^{m-n} b_{\ell^m} &= \sum_{k=0}^{\frac{\ell^n - \ell^m}{2}} (-1)^k \binom{\ell^n - \ell^m - k}{k} \binom{\ell^n - k - 1}{\ell^m - 1} t^{\ell^n - \ell^m - 2k} \\ &\equiv \sum_{k=0}^{\frac{\ell^n - \ell^m}{2}} (-1)^k \binom{\ell - k_m - 1}{k_m} \cdots \binom{\ell - k_{n-1} - 1}{k_{n-1}} t^{\ell^n - \ell^m - 2k} \\ &\equiv \prod_{j=m}^{n-1} \sum_{k_j=0}^{\frac{\ell-1}{2}} (-1)^{k_j} \binom{\ell - k_j - 1}{k_j} t^{\ell - 2k_j - 1} \\ &\equiv (U_{\ell-1}(t))^{n-m} \equiv \pm 1 \pmod{\ell}.\end{aligned}$$

The second to last step takes advantage of the fact that $t^{\ell^n - \ell^m} \equiv t^{\ell - 1} \equiv 1 \pmod{\ell}$, and the final step follows from Lemma 5.7. This concludes the proof. □

Remark 6. The assumption we made at the beginning of this section was that $t \not\equiv \pm 2 \pmod{\ell^2}$. However, in order to apply Lemma 5.7, we need to restrict t even further so that $t \equiv \pm 2 \pmod{\ell}$. However, since we are also assuming $\Phi(t) \equiv 0 \pmod{\ell^2}$, these conditions are equivalent thanks to Proposition 3.4. Specifically,

$$t \equiv \pm 2 \pmod{\ell^2} \quad \text{if and only if} \quad \left\{ \begin{array}{ll} t \equiv \pm 2 & \pmod{\ell}, \text{ and} \\ \Phi(t) \equiv 0 & \pmod{\ell^2} \end{array} \right\}.$$

Remark 7. We note that in this case, an alternative method for obtaining the ϕ-development is given by the Taylor expansion formula:

$$\Phi(x) = \Phi(t) + \Phi'(t)\phi(x) + \frac{1}{2}\Phi''(t)\phi(x)^2 + \cdots + \frac{1}{\ell^n!}\Phi^{(\ell^n)}(t)\phi(x)^{\ell^n}.$$

The result here is essentially identical to Proposition 5.3. In fact, what we have shown is that the Newton polygon of the Chebyshev polynomial $T_\ell^n(x)$ is invariant under shifts modulo the constant term. In particular, the ϕ-Newton polygon is ℓ-regular, and thus the Theorem of the Index (Theorem 4.6) gives an exact value for $\operatorname{ind}_\ell(\Phi)$. We provide a few examples at the end of this section to illustrate the formula.

Corollary 5.9. Let $v = \nu_\ell(\Phi(t))$. Let S_m be the edge connecting $(\ell^{m-1}, n-m+1)$ to $(\ell^m, n-m)$ and S' to be the edge connecting $(0, v)$ to $(\ell^{n-v+1}, v-1)$, as before. Then

$$N_\phi(\Phi) = S' + S_{n-v+2} + \cdots + S_n.$$

Moreover,

$$\operatorname{ind}_\ell(\Phi) = \sum_{i=1}^{\min\{v-1,n\}} \ell^{n-i}.$$

In particular, we have a precise formula for the discriminant of the number field in the following case.

Corollary 5.10. Suppose that $t+2$ and $t-2$ are square-free. Let $v = \nu_\ell(\Phi(t))$. Then

$$\Delta(K) = \frac{D(\Phi)}{\ell^{2\cdot\operatorname{ind}_\ell(\Phi)}}.$$

Example 5.11. Fix $t_0 = 3^6 \cdot 691 = 451251$. We note that $t_0 + 2$ and $t_0 - 2$ are square-free.

I. Consider the polynomial $T_3^3(x) - t_0$. By Theorem 3.6, $T_3(t) - t \equiv 0 \pmod 9$ if and only if $t \equiv 0, \pm 2 \pmod 9$. Since $\nu_3(t_0) = 6$, it is assured that $T_3^3(t_0) - t_0 \equiv 0 \pmod 9$. By Corollary 5.9,

$$\operatorname{ind}_\ell(T_3^3(x) - t_0) = \sum_{i=1}^{3} 3^{3-i} = 13,$$

and by Corollary 5.10,

$$\Delta(K_{3,3,t_0}) = \frac{3^{81}(4-t_0^2)^{13}}{3^{26}} = 3^{55}(4-t_0^2)^{13}.$$

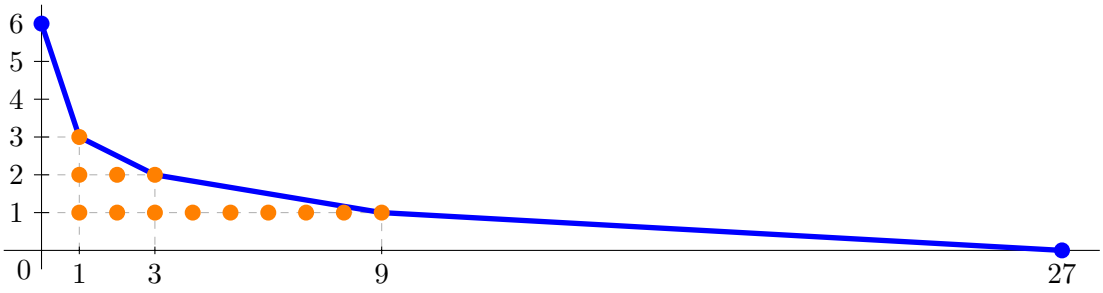

FIGURE 2. The ϕ-Newton polygon for $T_3^3(x) - t_0$ with $\phi(x) = x$. The polynomial ϕ is determined by reducing $T_3^3(x) - t_0$ modulo 3: $T_3^3(x) - t_0 \equiv x^{27} \pmod 3$. The 3-index is computed by counting the integral points lying below the polygon.

II. Consider the polynomial $T_5^3(x) - t_0$. By Theorem 3.6, $T_5(t) - t \equiv 0 \pmod{25}$ if and only if $t \equiv 0, \pm 1, \pm 2 \pmod{25}$, and we note that $t_0 \equiv 1 \pmod{25}$. Moreover, $\nu_5(T_5^3(t_0) - t_0) = 4$, so by Corollary 5.9,

$$\operatorname{ind}_5(T_5^3 - t_0) = \sum_{i=1}^{3} 5^{3-i} = 31,$$

and by Corollary 5.10,

$$\Delta(K_{5,3,t_0}) = \frac{5^{375}(4 - t_0^2)^{62}}{5^{62}} = 5^{313}(4 - t_0^2)^{62}.$$

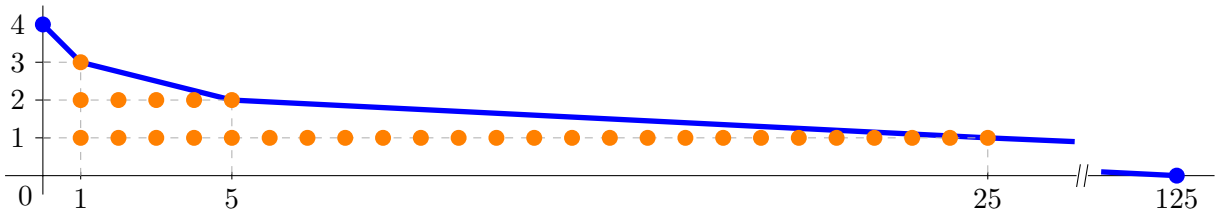

FIGURE 3. The ϕ-Newton polygon for $T_5^3(x) - t_0$ with $\phi(x) = x + 1$. The polynomial ϕ is determined by reducing $T_5^3(x) - t_0$ modulo 5: $T_5^3(x) - t_0 \equiv (x+1)^{125} \pmod{5}$.

III. Consider the polynomial $T_7^3(x) - t_0$. Note that $\nu_7(T_7^3(t_0) - t_0) = 2$. By Corollary 5.9,

$$\operatorname{ind}_7(T_7^3(x) - t_0) = \sum_{i=1}^{1} 7^{3-i} = 49,$$

and by Corollary 5.10,

$$\Delta(K_{7,3,t_0}) = \frac{7^{1029}(4 - t_0^2)^{171}}{7^{98}} = 7^{931}(4 - t_0^2)^{171}.$$

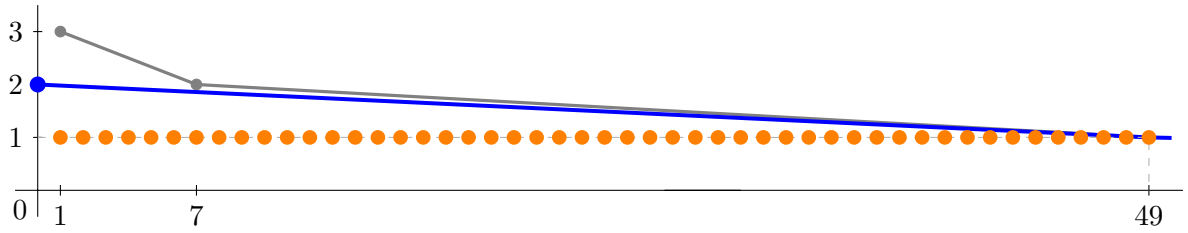

FIGURE 4. The ϕ-Newton polygon of $T_7^3(x) - t_0$ where $\phi(x) = x + 3$. The gray line indicates the ϕ-Newton polygon of $T_7^3(x) - t_0$ before considering the constant term of the ϕ-development. The end vertex of the polygon (343,0) is not shown.

6. Index calculations: On the multiplicity of p

In the proof of Theorem 3.3, we showed that for primes $p \neq \ell$, $\mathbb{Z}[\theta]$ is p-maximal if and only if $t \not\equiv \pm 2 \pmod{p^2}$. In this section, we consider $\operatorname{ind}_p(\Phi)$ when p is an odd prime different from ℓ. Specifically, we assume throughout this section that $t \not\equiv \pm 2 \pmod{\ell^2}$, and for convenience, we also assume that t is odd to avoid the special cases that arise when 2 divides $t^2 - 4$. The problem, under these conditions, appears to be slightly less tractable. However, we do provide conjectures for $\operatorname{ind}_p(\Phi)$, as well as a discussion on how we arrived at our formula and a case where the conjectures hold.

Conjecture 6.1. If $p \neq \ell$ is an odd prime for which $t \equiv \pm 2 \pmod{p^2}$, then

$$\nu_p(\mathrm{ind}(\Phi)) := \mathrm{ind}_p(\Phi) = \left\lfloor \frac{\nu_p(t^2-4)}{2} \right\rfloor \frac{\ell^n - 1}{2}.$$

We arrive at this conjecture largely through computational evidence. The main difficulty in applying the Montes algorithm to this case is satisfying the condition for regularity, as we will show. First, let $p \neq \ell$ be an odd prime, and recall that Φ factors modulo p as

$$\Phi(x) \equiv (x \pm 2)\phi_1(x)^2 \cdots \phi_r(x)^2.$$

A more detailed factorization was given in Proposition 2.3.

Let $\phi(x) := x \pm 2$.

Proposition 6.2. The factor $\phi(x) = x \pm 2$ makes no contribution to $\mathrm{ind}_p(\Phi)$, i.e. $\mathrm{ind}_\phi(\Phi) = 0$.

Proof. Since ϕ is linear, the ϕ-development is given by Taylor's expansion centered at ± 2:

$$\begin{aligned}\Phi(x) &= \Phi(\pm 2) + \Phi'(\pm 2)\phi(x) + \cdots \\ &= \Phi(\pm 2) + \ell^n U_{\ell^n - 1}(\pm 2)\phi(x) + \cdots .\end{aligned}$$

The following lemma allows us to compute $\nu_p(\ell^n U_{\ell^n-1}(\pm 2))$–the valuation of the coefficient of ϕ.

Lemma 6.3. $U_d(2) = d + 1$.

Proof. Recall that $U_0(x) = 1$ and $U_1(x) = x$, and the Chebyshev polynomials satisfy the relation $U_d(x) = xU_{d-1}(x) - U_{d-2}(x)$. The result follows by induction on d:

$$U_d(2) = 2U_{d-1}(2) - U_{d-2}(2) = 2(d) - (d-1) = d + 1.$$

□

Returning to the proof of the proposition, since U_{ℓ^n-1} is an even function, we see that $U_{\ell^n-1}(\pm 2) = \ell^n$. Therefore, the ϕ-Newton polygon is (at most) one-sided with vertices $\big(0, \nu_p(\Phi(\pm 2))\big)$ and $(1, 0)$. In particular, there are no integral points in the region bounded by this edge. The slope of this side is enough to conclude that Φ is ϕ-regular, and thus $\mathrm{ind}_\phi(\Phi) = 0$. □

We now consider the contributions of the other factors of $\overline{\Phi}$. Fix an irreducible factor ϕ_i of $\overline{\Phi}$ (different from $x \pm 2$) and let $\hat{\phi}_i$ be an arbitrary lift of ϕ_i. The $\hat{\phi}_i$-development of Φ is

$$\Phi(x) = a_0(x) + a_1(x)\hat{\phi}_i(x) + a_2(x)\hat{\phi}_i(x)^2 + \cdots , \tag{6.1}$$

and since $\overline{\Phi}$ is divisible by $\phi_i(x)^2$, we see that $\nu_p(a_2(x)) = 0$, $\nu_p(a_1(x)) \geq 1$, and $\nu_p(a_0(x)) \geq 1$. Ideally, the resulting $\hat{\phi}_i$-polygon will either be two-sided, or one-sided with half-integer slope, as the corresponding residual polynomials would be degree 1, giving $\hat{\phi}_i$-regularity. However, finding a lift that yields one of these ideal polygons may be quite difficult. In fact, it may even be impossible to find a lift $\hat{\phi}_i$ for which Φ is $\hat{\phi}_i$-regular. It turns out, though, that satisfying the regularity condition may be more than we need.

Conjecture 6.4. Let p be an odd prime. For each irreducible factor ϕ_i of Φ modulo p, there exists a lift $\hat{\phi}_i$ such that the corresponding $\hat{\phi}_i$-Newton polygon is one-sided with vertices $(0, \nu_p(\Phi(t))$ and $(2, 0)$.

In fact, Conjecture 6.4 implies Conjecture 6.1: Assume that we can always find such a lift. If $\nu_p(t^2-4)$ is odd, then as noted above, Φ is p-regular, and by Theorem 4.6 we have

$$\mathrm{ind}_p(\Phi) = \sum_{i=1}^{r} \mathrm{ind}_{\hat{\phi}_i}(\Phi) = \sum_{i=1}^{r} \left\lfloor \frac{\nu_p(t^2-4)}{2} \right\rfloor \cdot \deg(\hat{\phi}_i) = \left\lfloor \frac{\nu_p(t^2-4)}{2} \right\rfloor \cdot \frac{\ell^n - 1}{2}.$$

Otherwise, if $\nu_p(t^2-4)$ is even, then we cannot guarantee that Φ is p-regular. However, $\mathrm{ind}_p(\Phi)$ is bounded above by the valuation of the discriminant of Φ, and once again, we have equality.

$$\sum_{i=1}^{r} \mathrm{ind}_{\hat{\phi}_i}(\Phi) = \frac{\nu_p(t^2-4)}{2} \cdot \frac{\ell^n-1}{2} \leq \mathrm{ind}_p(\Phi) \leq \left\lfloor \frac{\nu_p(D(\Phi))}{2} \right\rfloor = \frac{\nu_p(t^2-4)}{2} \cdot \frac{\ell^n-1}{2}.$$

Moreover, this conjecture implies that (other than ℓ) the only primes that ramify in K are the primes that divide t^2-4 to an odd power. That is, we have the following discriminant formula for K:

Conjecture 6.5. Suppose t is odd and $t \not\equiv \pm 2 \pmod{\ell^2}$, and write $t^2-4 = A^2B$ where B is square-free. Then

$$\Delta(K) = \ell^{n\ell^n - 2\cdot \mathrm{ind}_\ell(\Phi)} B^{(\ell^n-1)/2}$$

where $\mathrm{ind}_\ell(\Phi)$ is given by Corollary 5.9.

In special cases we can guarantee that these conjectures hold. Recall from Proposition 2.3 that we defined μ to be the minimal positive integer for which $\nu_\ell(p^{2\mu}-1) \geq 1$, and $h := \nu_\ell(p^{2\mu}-1)$. Let p be a prime for which $\mu = (\ell-1)/2$ and $h = 1$, and suppose $t \equiv \pm 2 \pmod{p^2}$. For the remainder of this discussion, we choose the representative $\overline{t} \in \{-2, 2\}$ for the reduction of t modulo p. By Proposition 2.3, $T_\ell^n(x) - t$ factors modulo p as

$$T_\ell^n(x) - t \equiv (x - \overline{t}) \prod_{k=0}^{n-1} \psi(T_\ell^k(x))^2 \pmod{p},$$

where $\psi(T_\ell^k(x))$ is a monic polynomial of degree $\ell^k(\ell-1)/2$. Recalling the factorization of $T_\ell^n(x) - \overline{t}$ from Lemma 2.1, we see that each factor $\psi(T_\ell^k(x))$ lifts to the irreducible factor $\phi_{k+1}(x)$ of $T_\ell^n(x) - \overline{t}$. Using this factorization, we write

$$T_\ell^n(x) - t = T_\ell^n(x) - \overline{t} + (\overline{t} - t) = (\overline{t} - t) + (x - \overline{t})\phi_1(x)^2 \cdots \phi_n(x)^2,$$

from which we get a decomposition for each of the factors that satisfies Conjecture 6.4. We have proven the following:

Proposition 6.6. Let $\Phi(x) = T_\ell^n(x) - t$ as before, and let p be a prime for which $t \equiv \pm 2 \pmod{p}$. If $\mu = (\ell-1)/2$ is the minimal positive integer for which $\nu_\ell(p^{2\mu}-1) = 1$, then

$$\mathrm{ind}_p(\Phi) = \left\lfloor \frac{\nu_p(t^2-4)}{2} \right\rfloor \cdot \frac{\ell^n-1}{2}.$$

We illustrate the ideas in this section with the following example.

Example 6.7. Let $t_0 = 7^7 \cdot 11^4 \cdot 127^2 + 2$, and consider the polynomial $\Phi(x) = T_5^2(x) - t_0$. We note the prime factorization of $t_0^2 - 4$:

$$t_0^2 - 4 = 7^7 \cdot 11^4 \cdot 53 \cdot 127^2 \cdot 487 \cdot 499 \cdot 15099379,$$

hence $\mathrm{ind}(\Phi)$ is divisible by 7, 11, and 127. Theorem 3.6 eliminates the possibility that 5 divides $\mathrm{ind}(\Phi)$ since $t_0 \not\equiv 0, \pm 1, \pm 2 \pmod{25}$, thus 7, 11, and 127 are the only primes dividing $\mathrm{ind}(\Phi)$.

Case $p = 7$: The factorization of Φ modulo 7 has six irreducible factors of degree 2.

$$\Phi(x) \equiv (x-2) \prod_{i=1}^{6} \phi_{7,i}(x)^2 \pmod{7} \qquad \text{where}$$

$$\phi_{7,1}(x) = x^2 + x - 1 \qquad\qquad \phi_{7,4}(x) = x^2 - 3x - 2$$

$$\phi_{7,2}(x) = x^2 + 2x + 2 \qquad \phi_{7,5}(x) = x^2 - 2x + 3$$
$$\phi_{7,3}(x) = x^2 - 3x + 1 \qquad \phi_{7,6}(x) = x^2 - x + 3.$$

(We have adopted the notation of taking coefficients in $[-3, 3]$.) As noted above, the $x - \overline{t}_0$ term does not affect $\mathrm{ind}_7(\Phi)$, and so we only need to focus on the quadratic factors. For the factor $\phi_{7,1}$, we can use the factorization of $T_5(x) - 2$ to obtain a decomposition. We have

$$T_5(x) - t_0 = T_5(x) - 2 + (2 - t_0) = (x - 2)(x^2 + x - 1)^2 + (2 - t_0),$$

thus

$$\begin{aligned}\Phi(x) = T_5^2(x) - t_0 = T_5(T_5(x)) - t_0 &= (T_5(x) - 2)\left(T_5(x)^2 + T_5(x) - 1\right)^2 + (2 - t_0) \\ &= (x - 2)(x^2 + x - 1)^2\left(T_5(x)^2 + T_5(x) - 1\right)^2 + (2 - t_0).\end{aligned}$$

Following the notation from Equation (6.1), we have $\nu_7(a_0(x)) = \nu_7(2-t) = 7$, $\nu_7(a_1(x)) = \nu_7(0) = \infty$, and $\nu_7(a_2(x)) = 0$. Thus the associated $\phi_{7,1}$-polygon is one-sided with vertices (0,7) and (2,0). This method does not apply to the other factors, so we just give lifts that satisfy Conjecture 6.4. (See Figure 5.)

$\hat{\phi}(x) = x^2 + (a_1 + 7k_1)x + (a_0 + 7k_0)$	(k_1, k_0)
$\hat{\phi}_{7,1}(x) = x^2 + x - 1$	$(0, 0)$
$\hat{\phi}_{7,2}(x) = x^2 + 2354x + 457$	$(336, 65)$
$\hat{\phi}_{7,3}(x) = x^2 + 1110x + 2178$	$(159, 311)$
$\hat{\phi}_{7,4}(x) = x^2 + 1572x + 47$	$(225, 7)$
$\hat{\phi}_{7,5}(x) = x^2 + 1944x + 1291$	$(278, 184)$
$\hat{\phi}_{7,6}(x) = x^2 + 223x + 829$	$(32, 118)$

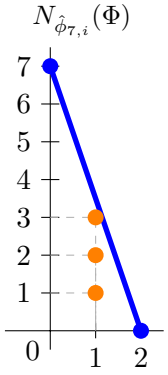

FIGURE 5. The pairs (k_1, k_0) are the least positive integers providing a desired lift. In fact, these values are unique modulo 7^3.

Case $p = 11$: Φ has the following factorization modulo 11.

$$\Phi(x) = (x - 2)\prod_{i=1}^{4}\phi_{11,i}(x)^2 \pmod{11} \qquad \text{where}$$

$$\phi_{11,1}(x) = x + 4 \qquad \phi_{11,3}(x) = \phi_{11,1}(T_5(x)) = x^5 - 5x^3 + 5x + 4$$
$$\phi_{11,2}(x) = x - 3 \qquad \phi_{11,4}(x) = \phi_{11,2}(T_5(x)) = x^5 - 5x^3 + 5x - 3.$$

Lifts satisfying Conjecture 6.4 are given in Figure 6. We note that the lifts for the linear factors also give desired developments for the polynomial $T_5(x) - t_0$. This is significant because the $\hat{\phi}_{11,1}$-development for $T_5(x) - t_0$ gives the $\hat{\phi}_{11,3}$-development for $\Phi(x) = T_5(T_5(x)) - t_0$, and similarly, the $\hat{\phi}_{11,2}$-development for $T_5(x) - t_0$ gives the $\hat{\phi}_{11,4}$-development for Φ.

Case $p = 127$: The prime 127 satisfies the conditions in Proposition 6.6, hence good lifts are given by the factorization of Φ in $\mathbb{Z}[x]$.

Since the desired lifts exist for each of the factors, we have determined the discriminant of K.

$$\Delta(K) = 5^{50}\left(7 \cdot 53 \cdot 487 \cdot 499 \cdot 15099379\right)^{12}.$$

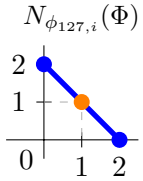

FIGURE 7

$\hat{\phi}(x) = x + (a_0 + 11k_0)$	k_0
$\hat{\phi}_{11,1}(x) = x + 37$	3
$\hat{\phi}_{11,2}(x) = x + 85$	8
$\hat{\phi}_{11,3}(x) = T_{\overline{5}}(x) + 37$	3
$\hat{\phi}_{11,4}(x) = T_{\overline{5}}(x) + 85$	8

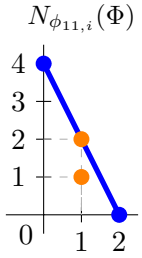

FIGURE 6. These values for k_0 are unique modulo 11.

7. Integral basis

The Montes algorithm also provides an efficient method for determining an integral basis for the ring of integers $\mathcal{O}_K$. In this section we summarize their procedure as it pertains to our situation.

For this discussion we assume that Φ is regular with respect to every prime. Fix a prime p for which $\mathbb{Z}[\theta]$ is not maximal. Let $\hat{\phi}_i$ be a lift of an irreducible factor of $\overline{\Phi}$ for which Φ is $\hat{\phi}_i$-regular. We define the quotients attached to the $\hat{\phi}_i$-developement of Φ to be the polynomials

$$\begin{aligned}
\Phi(x) &= \hat{\phi}_i(x)q_{i,1}(x) + a_{i,0}(x) \\
q_{i,1}(x) &= \hat{\phi}_i(x)q_{i,2}(x) + a_{i,1}(x) \\
&\vdots \\
q_{i,r-1}(x) &= \hat{\phi}_i(x)q_{i,r}(x) + a_{i,r-1}(x) \\
q_{i,r}(x) &= a_{i,r}(x).
\end{aligned}$$

Additionally, for $1 \le j \le r$, we identify the points $(j, y_{i,j})$ on the polygon $N_{\hat{\phi}_i}(\Phi)$.

Corollary 7.1. The collection $\{q_{i,j}(\theta)/p^{\lfloor y_{i,j} \rfloor}\}$ contains a p-integral basis for $\mathcal{O}_K$.

Proof. This is a specialization of [3], Theorem 2.6. □

In section 5, we precisely determined the ϕ-polygon for Φ for certain values of t. Under these same conditions, we determine generators for the ring $\mathcal{O}_K$.

Proposition 7.2. Suppose that $t-2$ and $t+2$ are square-free, $\Phi(t) \equiv 0 \pmod{\ell^2}$, and $t \not\equiv \pm 2 \pmod{\ell^2}$. Let $v = \min\{\nu_\ell(\Phi(t)) - 1, n\}$. Then

$$\mathcal{O}_K = \mathbb{Z}\left[\theta, \frac{q_{\ell^{n-1}}(\theta)}{\ell}, \frac{q_{\ell^{n-2}}(\theta)}{\ell^2}, \ldots, \frac{q_{\ell^{n-v}}(\theta)}{\ell^v}\right].$$

Proof. Recall that $\Phi(x) = T_\ell^n(x) - t \equiv (x-t)^{\ell^n} \pmod{\ell}$, so let $\phi(x) = x - \overline{t}$. In Corollary 5.9 we determined $N_\phi(\Phi)$ and showed that Φ is ℓ-regular. For each $1 \le j \le \ell^n$, the quotient $q_j(x)$ is a monic polynomial of degree $\ell^n - j$, and these quotients satisfy the recursion $q_j(x) = \phi(x)q_{j+1}(x) + a_j$ where $q_{\ell^n}(x) = 1$. By definition, $\nu_\ell(a_j) \ge \lfloor y_j \rfloor$. Hence if $\lfloor y_{j+1} \rfloor = \lfloor y_j \rfloor$, then $q_{j+1}(\theta)/\ell^{\lfloor y_{j+1} \rfloor} \in \mathcal{O}_K$ implies that $q_j(\theta)/\ell^{\lfloor y_j \rfloor} \in \mathcal{O}_K$. It follows that

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{q_{\ell^n}(\theta)}{\ell^{\lfloor y_{\ell^n} \rfloor}}, \ldots, \frac{q_1(\theta)}{\ell^{\lfloor y_1 \rfloor}}\right] = \mathbb{Z}\left[\theta, \frac{q_{\ell^{n-1}}(\theta)}{\ell}, \frac{q_{\ell^{n-2}}(\theta)}{\ell^2}, \ldots, \frac{q_{\ell^{n-v}}(\theta)}{\ell^v}\right].$$

□

References

[1] W. Aitken, F. Hajir, and C. Maire. Finitely ramified iterated extensions. *IMRN*, 14:855–880, 2005.

[2] H. Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics. Springer, 1995.

[3] L. el Fadil, J. Montes, and E. Nart. Newton polygons and p-integral bases, 2009. arXiv:09062629v1 [math.NT].

[4] T. A. Gassert. Chebyshev action on finite fields, 2012. arXiv:1209.4396.v2 [math.NT].

[5] J. Guàrdia, J. Montes, and E. Nart. Higher newton polygons in the computation of discriminants and prime ideal decomposition in number fields. *J. Théo. Nombres Bordeaux*, 23(3):667–696, 2011.

[6] J. Guàrdia, J. Montes, and E. Nart. Higher newton polygons and integral bases, 2012. arXiv:0902.3428v3 [math.NT].

[7] J. Guàrdia, J. Montes, and E. Nart. Newton polygons of higher order in algebraic number theory. *Trans. Amer. Math Soc.*, 364(1):361–416, 2012.

[8] E. Kummer. Über die ergänzungssätze zu den allgemeinen reziprokcitäusgesetzten. *Journal für die reine und angewandte Mathematik*, 44:93–146, 1852.

[9] E. Lucas. Sur les congruences des nombres eulériens et les coefficients différentiels des functions trigonométriqués suivant un module premier. *Bulletin de la Société Mathématique de France*, 6:49–54, 1878.

[10] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. Springer Monographs in Mathematics. Springer, 2004.

[11] T. J. Rivlin. *Chebyshev Polynomials: From Approximation Theory to Algebra and Number Theory*. Pure and Applied Mathematics. Wiley, 1990.

[12] J. Silverman. *The Arithmetic of Dynamical Systems*. Graduate Texts in Mathematics. Springer, 2007.

E-mail address: gassert@math.umass.edu

Department of Mathematics and Statistics, University of Massachusetts, Amherst, 710 N. Pleasant Street, Amherst, MA, USA 01003